

# Avoid ID Theft

**How to Deter, Detect, and Defend  
Against Identity Theft**

# Identity Theft

8.4 Million Americans  
\$49.3 Billion in losses  
\$587 Out-of-pocket costs  
40 hours of your time to resolve  
53% of known thieves - *were known by the victim!*





DETER



DETECT



DEFEND

## what is identity theft?

- It occurs when someone steals your personal information e.g., credit card or Social Security number – and uses it fraudulently
- It can cost you time and money
- It can destroy your credit and ruin your good name

DETER·DETECT·DEFEND

**AVOID** THEFT

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**VISA**

FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | [FTC.GOV/IDTHIFT](http://FTC.GOV/IDTHIFT) | 1-877-ID-THEFT (438-4338)

# What can you do?



## DETER

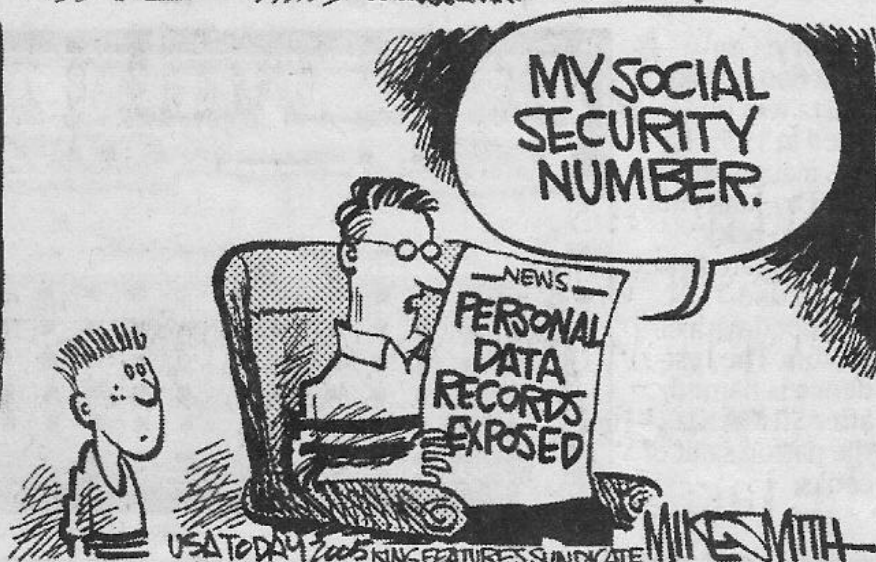
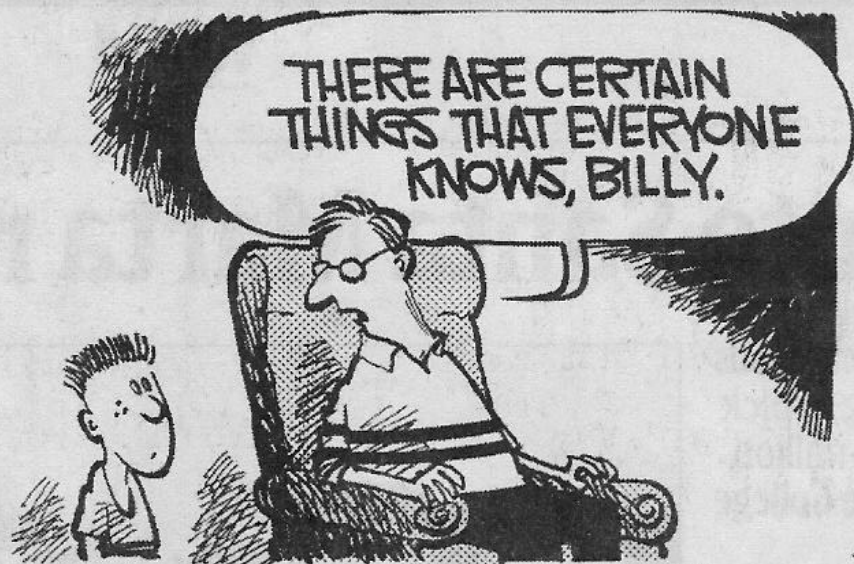
- Deter identity thieves by safeguarding your information

## DETECT

- Detect suspicious activity by routinely monitoring your financial accounts and billing statements

## DEFEND

- Defend against identity theft as soon as you suspect a problem



By Mike Smith, Las Vegas Sun, for USA TODAY

## Letters



DETER



DETECT



DEFEND

# How does identity theft happen?

Identity thieves may:

- Go through your trash or “dumpster dive”
- Steal your wallet or purse
- Steal your mail and/or submit a change of address form for your mail

DETER • DETECT • DEFEND

**AVOID** THEFT

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**VISA**

FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | [FTC.GOV/IDTHEFT](http://FTC.GOV/IDTHEFT) | 1-877-ID-THEFT (438-4338)



DETER



DETECT



DEFEND

# How does identity theft happen?

Identity thieves may:

- Use “phishing” or fake emails to get you to provide personal information
- Steal personnel records from their employers
- Obtain personal information from your computer

DETER • DETECT • DEFEND



[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)



FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | [FTC.GOV/IDTHEFT](http://FTC.GOV/IDTHEFT) | 1-877-ID-THEFT (438-4338)



DETER



DETECT



DEFEND

## How does identity theft happen?

Identity thieves may:

- They get your information from the businesses in a practice known as “business record theft” (customer, employee, patient or student; bribing an employee who has access to your files; or “hacking” into electronic files).

DETER • DETECT • DEFEND

**AVOID** THEFT

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

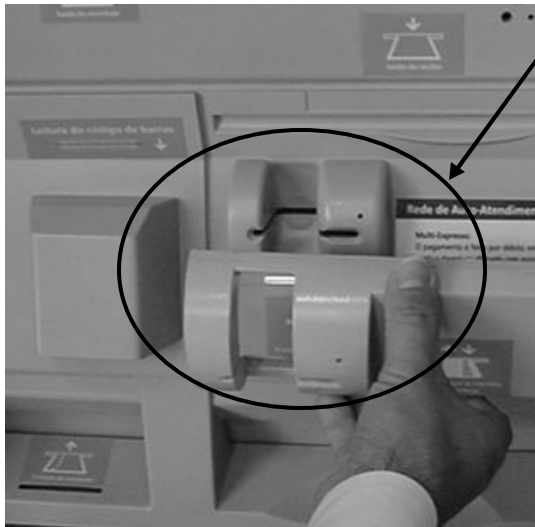
**VISA**

FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | [FTC.GOV/IDTHEFT](http://FTC.GOV/IDTHEFT) | 1-877-ID-THEFT (438-4338)



# They skim or otherwise obtain your card information

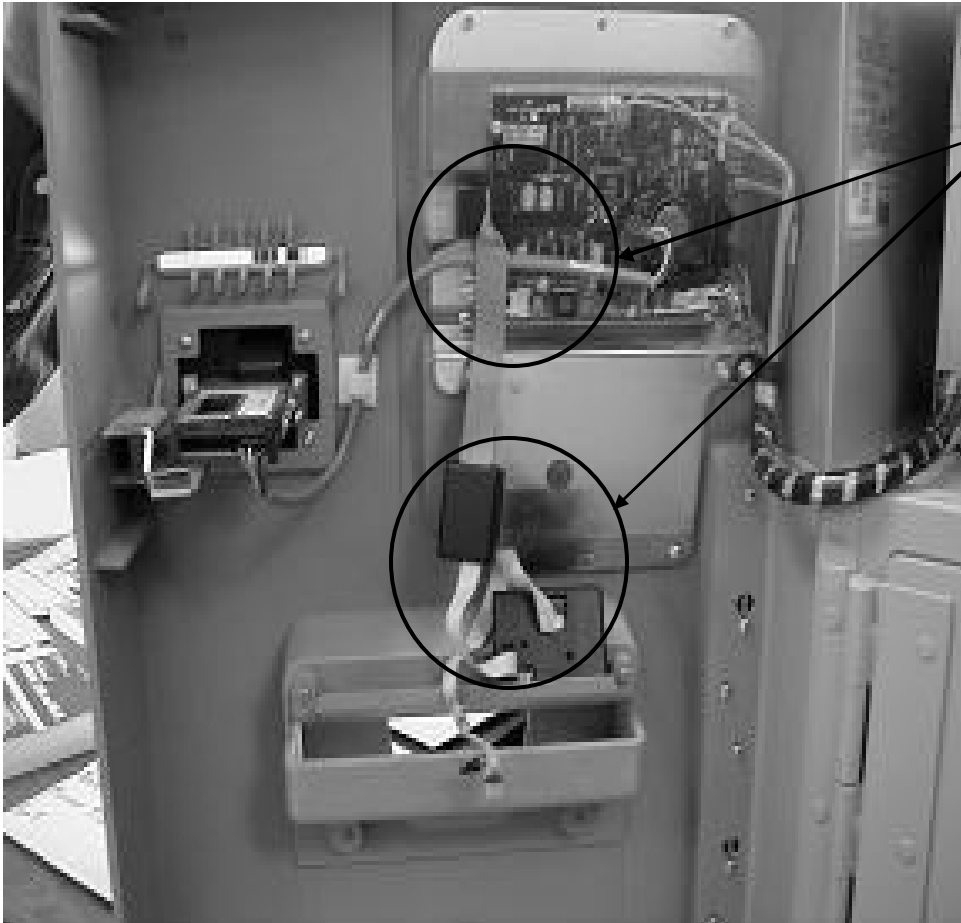
**VISA**



- False fronts on ATM terminals with built in magnetic stripe readers.
- Hidden camera captures PIN and transmits the information to a nearby crook
- Increasingly common



## ATM – Environment – Cont'd



- **Sniffing devices installed in ATMs are another example of how a fraudster can compromise the ATM or Debit card PIN. In this example, the PIN and magnetic stripe information are captured before encryption.**
- **Recent cases have Bluetooth transmission to remote receiver.**

# And An Old Favorite – “The Skimmer”

**VISA**



- This device can capture over 2500 credit card account numbers, expiration dates and CVV codes in the palm of your hand.
- The unit can operate continuously for 40 hours on a single 3V battery (6000 swipes).
- Skimmed data can be downloaded to any PC with software provided.
- At a moment's notice, or the moment of arrest, the contents can be deleted with the press of a button to avoid prosecution.
- Cost = \$500

They get your information from the businesses...  
“hacking” into electronic files.



**DAILY BRIEFING**  
**May 1, 2006**

### Hackers access personal information on TRICARE servers

**By Daniel Pulliam**  
**[dpulliam@govexec.com](mailto:dpulliam@govexec.com)**

Hackers gained access to the Pentagon's health insurance information systems, compromising the personal information of more than 14,000 people...

The intrusion of the TRICARE Management Activity public computer servers was discovered on April 5...The hacked information included databases of names, Social Security numbers, the last four digits of credit card numbers, personal phone numbers, work and personal e-mail addresses and home addresses.

The Defense Criminal Investigative Service is participating in an investigation of the incident.

The department sent affected people letters informing them that the compromise of their personal information could put them at risk for identity theft and recommending precautionary measures.

"A security problem of this magnitude on this level underscores the need to address security as a fundamental issue on the development and implementation of any national electronic health care record initiative," McNulty said.

# Phishing



- 73 Million adult email users reported more than 50 phishing emails during 2006
- 11 million recipients of phishing emails clicked on the links
- 2.42 million adults reported losing money because of phishing attacks (\$929 million)
- Pay Pal and E bay are the top spoofed sites. Citibank is the primary bank target for phishing scams



# Expected Phishing!!

Dear Taxpayer

We have received your tax filing and are prepared to send your refund. However, we are experiencing difficulty in timely forwarding you refund to your bank and need your assistance.

Do not respond to this email for security purposes.

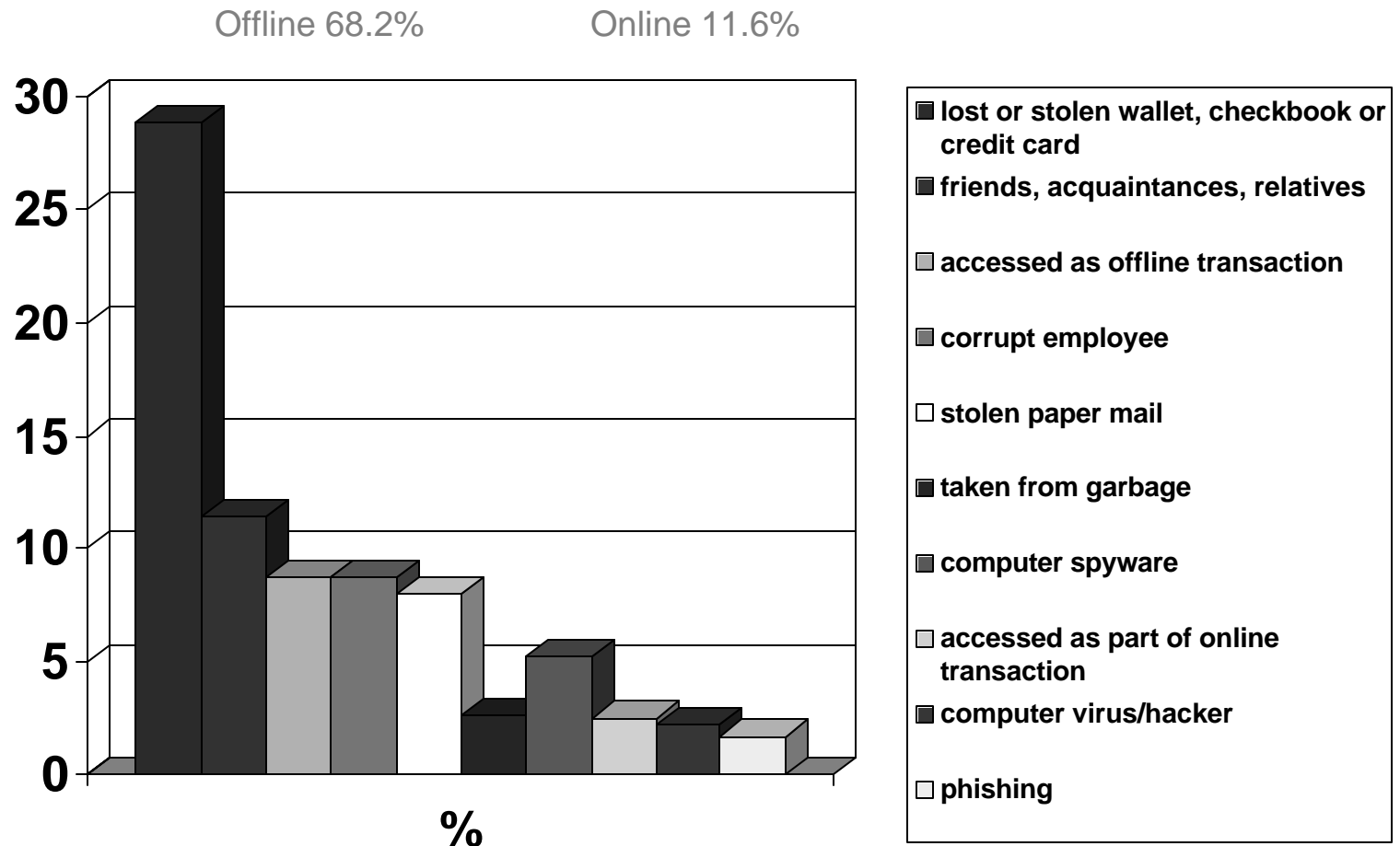
Go to our secure website at <https://www.irs.gov/payments> to complete the information required so we can forward your tax refund.



# Is it Phishing?

1. Does the email ask you to go to a website and verify personal information? Banks won't ask you to verify your personal information in response to an email.
2. What is the tone of the mail? Most phish emails convey a sense of urgency by threatening discontinued service or information loss if you don't take immediate action.
3. What is the quality of the email? Many phish emails have misspellings, bad grammar, or poor punctuation.
4. Are the links in the email valid? Deceptive links in phishing emails look like they are to a valid site, but deliver you to a fraudulent one. Many times you can see if the link is legitimate by just moving your mouse over the link.
5. Is the email personalized with your name and applicable account information? Many phish emails use generic salutations and generic information (e.g. Dear Customer or Dear Account Holder) instead of your name.
6. What is the sender's email address? Many phish emails come from an email address not from the company represented in the email.
7. When in doubt, type it out. If you suspect an email to be phishing, don't click on any links in the email. Type the valid address directly into your web browser.

# Offline Versus Online Methods of Access Causes Of Known Theft







DETER



DETECT



DEFEND

## DETER identity thieves by safeguarding your information.

- Shred financial documents before discarding them
- Protect your Social Security number
- Don't give out personal information unless you're sure who you're dealing with

DETER • DETECT • DEFEND

**AVOID** THEFT

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**VISA**

FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | [FTC.GOV/IDTHIFT](http://FTC.GOV/IDTHIFT) | 1-877-ID-THEFT (438-4338)



DETER



DETECT



DEFEND

## DETER identity thieves by safeguarding your information.

- Don't use obvious passwords
- Keep your information secure
- Use a Firewall, Virus Protection, Anti-Spyware Software
- Carry only the identification information and credit and debit cards that you'll actually need.

DETER • DETECT • DEFEND

**AVOID** THEFT

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**VISA**

FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | [FTC.GOV/IDTHIFT](http://FTC.GOV/IDTHIFT) | 1-877-ID-THEFT (438-4338)

Are you Safe?  
Take the Test!



[www.idsafety.net](http://www.idsafety.net)



**DETER**



**DETECT**



**DEFEND**

**DETECT** suspicious activity by routinely monitoring your financial accounts and billing statements.

- Be alert
  - Mail or bills that don't arrive
  - Denials of credit for no reason
- Inspect your financial statements
  - Look for charges you didn't make

DETER • DETECT • DEFEND

**AVOID** THEFT

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | [FTC.GOV/IDTHEFT](http://FTC.GOV/IDTHEFT) | 1-877-ID-THEFT (438-4338)

**VISA**



**DETER**



**DETECT**



**DEFEND**

**DETECT** suspicious activity by routinely monitoring your financial accounts and billing statements.

- Inspect your credit report
    - Law entitles you to one free report a year from each Nationwide credit reporting agencies if you ask for it
- Online: [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com);  
by phone: 1-877-322-8228;  
or by mail: Annual Credit Report Request Service,  
P.O. Box 105281, Atlanta, GA 30348-5281

DETER • DETECT • DEFEND



[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)



FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | [FTC.GOV/IDTHIFT](http://FTC.GOV/IDTHIFT) | 1-877-ID-THEFT (438-4338)



**DETER**



**DETECT**



**DEFEND**

**DEFEND** against identity theft as soon as you suspect a problem.

- Contact Fraud Department of Creditors.
- Review reports carefully, looking for fraudulent activity
- Close accounts that have been tampered with or opened fraudulently
- File a police report
- Place a “Fraud Alert” on your credit reports
- Contact the Federal Trade Commission

DETER • DETECT • DEFEND

**AVOID** THEFT

**VISA**



DETER



DETECT



DEFEND

## WHERE CAN YOU LEARN MORE?

Online: [ftc.gov/idtheft](https://ftc.gov/idtheft)

By phone: 1-877-ID-THEFT

By mail: Identity Theft Clearinghouse  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

DETER • DETECT • DEFEND



[www.ftc.gov/idtheft](https://www.ftc.gov/idtheft)



FEDERAL TRADE COMMISSION | 600 PENNSYLVANIA AVE., NW WASHINGTON, DC 20580 | [FTC.GOV/IDTHEFT](https://FTC.GOV/IDTHEFT) | 1-877-ID-THEFT (438-4338)

Are you a Victim?  
Professional help available!



1-866-ID-HOTLINE, victims can receive free and confidential assistance from trained counselors.



# What's Visa doing?

## Card Technological Safeguards

